Amendments to the Specification

Please replace the paragraph on Page 2 beginning on line 21 and continuing to Page 3, line 7 with the following amended paragraph:

In accordance with this invention there is provided a method for generating a shared secret value between entities in a data communication system, one or more of the entities having a plurality of members for participation in the communication system, each member having a long term private key and a corresponding long term public key, the method comprising the steps of:

(a) generating an entity long term public key for each entity by combining the long term public keys of each members of the entity.

(b) generating a short term private and a corresponding short term public key for each of the members;

(c) making said short term public key available to members within an entity;

(d) for each member:

  (i) computing an intra-entity shared key by mathematically combining said short term public keys of each said member;

  (ii) computing an intra-entity public key by mathematically combining its short-term private key, the long term private key and said intra-entity shared key;

(e) for each entity combining intra-entity public keys to derive a group short-term public key;

(f) each entity making its intra-entity shared key and its entity long term public key available to said other entities; and

(g) each entity computing a common shared key K by combining its group short term public key, with the intra-entity shared key, and an entity long term public key received from the other entity.